네트워킹

Apple 정책 편집기의 네트워킹 섹션에서는 기기의 Wi-Fi 네트워크와 VPN을 구성하고, 인증서를 설치하며, AirDrop 및 Bluetooth와 같은 연결 기능을 제한합니다 . 각 Wi-Fi 네트워크, VPN 및 인증서는 자체 구성 프로필로 설치되며, 기기의 설정 > 일반 > VPN & 기기 관리 (Mac: 시스템 설정 > 일반 > 기기 관리, 또는 macOS 13 및 14에서는 개인 정보 보호 및 보안 > 프로필) 및 기기 페이지의 프로필, 인증서 및 보안 패널에서 확인할 수 있습니다.

인증서는 인증서 페이지에서 가져옵니다 . 먼저 해당 페이지에서 가져오세요 . 정책은 인증서를 참조만
하므로 정책에 인증서가 복사되지 않습니다.

제한
AirDrop 허용
AirPlay 수신 요청 허용
Bluetooth 수정 허용
Bluetooth 공유 수정 허용
파일 앱의 네트워크 드라이브 접근 허용
인터넷 공유 수정 허용
콘텐츠 캐싱 허용
iTunes 파일 공유 허용

Wi-Fi 네트워크
Wi-Fi 네트워크 추가 를 클릭하고 다음을 입력하세요 :

네트워크 이름 (SSID): 네트워크 이름이며 최대 32자입니다.
보안: 없음 (개방형 네트워크), WEP, WPA 또는 WPA2, WPA2 또는 WPA3, WPA3만, 또는 모두. 비밀번호 : 개인 네트워크의 비밀번호입니다 .
자동으로 연결 및 숨겨진 네트워크 (이름을 브로드캐스트하지 않는 네트워크용)입니다.
프록시: 없음, 수동 (서버 및 포트) 또는 자동 (PAC 파일 URL, 비워 두면 WPAD로 네트워크에서
설정을 찾음)입니다.
프로필 이름 (선택 사항) 및 적용 대상: 네트워크를 일부 기기 유형으로 제한합니다 .

엔터프라이즈 네트워크 (802.1X)

사용자가 공유 비밀번호 대신 자체 자격 증명이나 인증서로 인증하는 경우 엔터프라이즈 (802.1X)를 켜세요.

인증: PEAP, TTLS(내부 인증 포함, 예: MSCHAPv2) 또는 TLS(인증서만).
기기 사용자의 자격 증명: 각 기기는 사용자 페이지에서 설정한 사용자의 EAP ID, 익명 ID,
비밀번호를 사용합니다 . 사용자가 없는 기기에는 네트워크가 적용되지 않습니다.
ID, 익명 ID 및 비밀번호 : 모든 기기에 동일합니다 . ID에는 $EMAIL$, $USERNAME$,
$FULLNAME$, $SERIAL$, $UDID$ 변수를 포함할 수 있습니다. 비밀번호를 비워 두면 사용자가
기기에서 직접 입력합니다 .
ID 인증서: 기기가 제시하는 클라이언트 인증서입니다 (TLS에 필요). 아래 인증서 옵션을
참조하세요 .
신뢰할 수 있는 인증서: RADIUS 서버의 인증서를 발급한 CA 인증서입니다 . 네트워크와 함께
설치됩니다 .
신뢰할 수 있는 서버 이름: 기기가 허용하는 RADIUS 서버 인증서의 이름입니다 . 예: radius.example.com 또는 *.example.com.

VPN

VPN 추가 를 클릭하여 iOS, iPadOS, macOS에 내장된 IKEv2 또는 Cisco IPSec VPN을 구성하세요 (VPN 앱 필요 없음).

유형 및 서버. IKEv2의 경우 원격 ID(서버 ID, 비어 있으면 서버 주소)와 로컬 ID도 설정합니다 .
로컬 ID에는 $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$, $UDID$ 변수를 포함할 수
있습니다.
인증 (기기): 인증서 (인증서 페이지, 기기 사용자의 인증서, 또는 SCEP 서버에서 요청), 공유 비밀
(IPSec의 선택적 그룹 이름 포함), 또는 사용자 이름과 비밀번호만 확인하는 IKEv2 서버의 경우 없음

.

신뢰할 수 있는 인증서: VPN 서버의 CA 인증서이며 VPN과 함께 설치됩니다 . IKEv2의 경우 예상
서버 인증서 발급자와 이름도 설정할 수 있습니다.
사용자 이름 및 비밀번호 : 사용자는 사용자 이름 (변수 허용)과 비밀번호 (IKEv2는 EAP, IPSec은 XAuth)로도 인증합니다 . 비밀번호를 비워 두면 사용자가 기기에서 직접 입력합니다 .
VPN 이름 (설정에 표시됨) 및 적용 대상.

연결

사용자가 설정에서 연결: VPN이 설치되며 사용자가 필요할 때 켭니다.
요청 시: 기기가 VPN에 자동으로 연결합니다 . 신뢰할 수 있는 Wi-Fi 제외 를 사용하면 나열한 Wi-
Fi 네트워크 (예: 사무실 네트워크)에서는 VPN을 사용하지 않습니다.
상시 연결 (IKEv2, 감독되는 iPhone 및 iPad만 해당): 셀룰러와 Wi-Fi에서 모든 트래픽이 VPN을
통과하며 사용자가 끌 수 없습니다. 다른 기기에는 이 VPN이 적용되지 않습니다. VPN이 사용자
이름을 사용하는 경우 정책에 비밀번호를 설정해야 합니다.
앱별 VPN: 일부 앱만 VPN을 사용합니다 . 앱 관리 섹션에서 각 앱의 VPN을 선택하고 (앱의 VPN 필드, Mac에서는 사용할 수 없음), 선택적으로 이를 사용하는 Safari 도메인을 나열하세요 .

상시 연결 또는 요청 시 VPN은 먼저 테스트 기기에서 테스트하세요 . 서버에 연결할 수 없으면 기기가 연결되지 않을 수 있습니다.

전역 프록시, 암호화된 DNS 및 웹 콘텐츠 필터
이 설정은 기기의 모든 트래픽에 적용됩니다 . 해당 토글로 켜세요.

전역 HTTP 프록시 (감독되는 iPhone 및 iPad, Mac): 모든 HTTP 트래픽이 모든 네트워크에서
프록시를 통과합니다 . 서버와 포트 (선택적 사용자 이름 및 비밀번호 포함) 또는 자동 구성 (PAC 파일 URL, 비워 두면 네트워크에서 찾음)을 설정하세요 . Wi-Fi 로그인 페이지 허용 은 사용자가 프록시
없이 공용 Wi-Fi 네트워크에 로그인할 수 있게 합니다.
암호화된 DNS: 기기가 DNS over HTTPS(서버 URL) 또는 DNS over TLS(서버 이름)를 통해
사용자의 DNS 서버로 이름을 확인하며, 선택적으로 일부 도메인에만 적용할 수 있습니다. 감독되는 기기에서는 사용자가 이를 끄지 못하게 할 수 있습니다.
웹 콘텐츠 필터 (감독되는 iPhone 및 iPad): iOS에 내장된 필터가 성인 웹 사이트를 제한하며, 항상
허용 또는 항상 차단할 웹 사이트 목록을 사용하거나 웹 사이트 목록만 허용하고 Safari에 책갈피로
표시합니다 .

잘못된 프록시나 DNS 서버는 기기를 연결 불가 상태로 만들 수 있습니다. 먼저 테스트 기기에서
설정을 사용해 보세요.

인증서
인증서 추가 를 클릭하여 인증서를 단독으로 설치하세요 . Safari와 앱이 신뢰해야 하는 인증 기관이거나 앱이 사용하는 ID입니다. Wi-Fi 네트워크나 VPN의 인증서는 여기에 추가할 필요가 없습니다.

인증서 옵션

인증서 페이지의 인증서: 모든 기기에 동일한 인증서입니다 . 인증서 선택 을 클릭하여 선택하세요 .
기기 사용자의 인증서: 각 기기가 사용자와 연결된 클라이언트 인증서를 받습니다. 사용자에게
인증서가 없는 기기에는 적용되지 않습니다. 사용자에게 다른 인증서를 연결하면 기기가
업데이트됩니다 .
SCEP 서버에서 요청: 각 기기가 SCEP 서버 (예: Microsoft NDES)에서 자체 인증서를 요청하므로
개인 키가 기기를 떠나지 않습니다. 서버 URL, 서버가 요구하는 경우 챌린지, 주체 (예: CN=$EMAIL$), 대체 이름, 키 크기, 키 사용을 설정하세요 .

이전 RC2 암호화로 보호된 클라이언트 인증서 (.p12)는 Apple 기기에 설치할 수 없습니다. 가져오기
전에 3DES 또는 AES 암호화로 다시 내보내세요 .

보안
비밀번호나 개인 키가 포함된 프로필은 해당 프로필이 만들어진 기기에만 전송됩니다 . 기기는 관리 인증서로 요청에 서명해야 합니다. 비밀번호와 인증서는 로그에 기록되지 않습니다.

Revision #6
Created 2026-11-10 15:16:45 UTC by Admin
Updated 2026-11-12 09:56:29 UTC by Admin